REMARKS

The Examiner has rejected Claims 1, 10, 17, and 33 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicant respectfully asserts that such rejection is deemed avoided in view of the amendments made hereinabove to the claims.

Furthermore, the Examiner has rejected Claims 1, 3-6, 8-16, 17, 19-22, 24-32, 33, 35-38, and 40-47 under 35 U.S.C. 103(a) as being unpatentable over Lahti (U.S. Publication No. 2002/0042886 A1), in view of Hypponen (U.S. Patent No. 6,577,920 B1). Applicant respectfully disagrees with such rejection.

With respect to the independent claims, the Examiner has relied on the following excerpts from Lahti to make a prior art showing of applicant's claimed "generating from said master malware definition data said mobile computing device malware definition data, said mobile computing device malware definition data identifying items of malware identified within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected" (see this or similar, but not necessarily identical language in the independent claims).

> "Clearly, if effective protection is to be maintained, the database used by the anti-virus software must contain signatures for all known viruses. Unfortunately, new viruses are detected all the time, currently at the rate of one per day. Once a newly detected virus has been analysed by the anti-virus software provider and a signature created, the database must be updated on all of the computers which are using the anti-virus software. There have been various methods up until now for carrying out this update." (Paragraph [0003] - emphasis added)

> 'Increasingly, mobile phones are being used to connect to the Internet. Mobile Internet access is being facilitated by new networks (incorporating HSCSD and GPRS) as well as other protocols such as WAP. As mobile "platforms" with wireless modems and internet connections become more powerful, Internet connections will be as easy to obtain as for a desktop PC. This increase in the usage and capacity of mobile platforms renders

them susceptible to attack by viruses. The methods outlined above for updating...' (Paragraph [0005], lines 1-9 - emphasis added)

"It is, therefore, an object of the present invention to provide a means for updating anti-virus signature databases on mobile platforms." (Paragraph [0006] - emphasis added)

Applicant respectfully asserts that the excerpts relied upon by the Examiner merely teach that mobile phones are being used to connect to the Internet more frequently, and "[t]his increase in the usage and capacity of mobile platforms renders them susceptible to attack by viruses." Additionally, the excerpts teach that "if effective protection is to be maintained, the database used by the anti-virus software must contain signatures for all known viruses" and "[o]nce a newly detected virus has been analysed by the anti-virus software provider and a signature created, the database must be updated on all of the computers which are using the anti-virus software" (emphasis added). Furthermore, the excerpts state that "an object of the...invention [is] to provide a means for updating anti-virus signature databases on mobile platforms" (emphasis added).

However, Lahti's disclosure that anti-virus software must contain signatures for all known viruses and that the databases must be updated on the computers using the anti-virus software simply fails to suggest "mobile computing device malware definition data identifying items of malware identified within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected" (emphasis added), as claimed by applicant. Clearly, updating the anti-virus software with all virus definitions, as in Lahti, simply fails to even suggest "items of malware identified within said master malware definition data which are within classes of malware threat" (emphasis added), in the manner as claimed by applicant.

Additionally, with respect to the independent claims, the Examiner has relied on the following excerpts from Lahti to make a prior art showing of applicant's claimed technique "wherein said fixed location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed location computing device transfers computer files and corresponding threat data identifying one

or more classes of malware threat to which each of said mobile computing devices is vulnerable" (as amended, see this or similar, but not necessarily identical language in the independent claims).

> "...The anti-virus server 12 receives regular updates (e.g. every morning) from an update server 13 maintained by the anti-virus software provider. The SMS server 12 maintains a record of all subscribers to the anti-virus service in a database 13, and..." (Paragraph [0023], lines 4-8)
>
> "...initiates virus signature database updates by sending a Short Message Service (SMS) request for each of the registered subscribers (including the user of the mobile device 1) to the SMS centre 5." (Paragraph [0023], lines 9-12 - not specifically cited)

Applicant respectfully asserts that the excerpts relied upon by the Examiner merely teach that an update server is maintained by an anti-virus software provider. Further, Lahti discloses that the "SMS server 12 maintains a record of all subscribers to the anti-virus service in a database" and "initiates virus signature database updates by sending a Short Message Service (SMS) request for each of the registered subscribers."

However, Lahti's disclosure of a server that is maintained by an anti-virus service provider, and that the server initiates virus signature database updates to each registered subscriber, in no way suggests a technique "wherein said fixed location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed location computing device transfers computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable" (emphasis added), as claimed by applicant. Clearly, sending virus signature database updates to registered subscribers, as in Lahti, simply fails to even suggest "corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable" (emphasis added), in the manner as claimed by applicant.

Furthermore, with respect to the independent claims, the Examiner has relied on the following excerpt from Hypponen to make a prior art showing of applicant's claimed

"identifying one or more classes of malware threat against which said mobile computing device is to be protected" (see this or similar, but not necessarily identical language in the independent claims).

> "...if the file contains a macro, determining whether or not the macro has a signature corresponding to one of the signatures contained in said database.
>
> It will be appreciated that embodiments of the present invention have the advantage that they may be used to effectively block the transfer and/or processing of files which contain a previously unidentified (either to the local user or to the software producer) macro virus. It is therefore..." (Col. 2, lines 37-44 - emphasis added)

Applicant respectfully asserts that the excerpt relied upon by the Examiner merely teaches a method of screening a software file for viral infection which involves "determining whether or not the macro has a signature corresponding to one of the signatures contained in said database." In addition, the excerpt teaches "effectively block[ing] the transfer and/or processing of files which contain a previously unidentified (either to the local user or to the software producer) macro virus" (emphasis added).

However, Hypponen's disclosure of determining if the macro has a signature corresponding to a signature in a database, and blocking the transfer or processing of files containing an unidentified macro virus, in no way suggests "identifying one or more classes of malware threat against which said mobile computing device is to be protected" (emphasis added), as claimed by applicant. Clearly, blocking a transfer or processing a file containing an unidentified macro, as in Hypponen, simply fails to even suggest "identifying one or more classes of malware threat" (emphasis added), in the manner as claimed by applicant.

Still yet, with respect to the independent claims, the Examiner has relied on Col. 2, lines 27-63 from Hypponen to make a prior art showing of applicant's claimed technique "wherein only a subset of said master malware definition data is used to generate said mobile computing device malware definition data for tailoring said mobile computing device malware definition data to accommodate malware threats to which said

mobile computing device is vulnerable" (see this or similar, but not necessarily identical language in the independent claims).

Applicant respectfully asserts that the excerpt relied upon by the Examiner merely teaches that "said step of defining a database of signatures indicative of macros previously certified as being virus free comprises scanning a set of end user applications which are known to be virus free to identify macros therein, determining a signature for each of the identified macros, and compiling the determined signatures into the database" (Col. 2, lines 47-52 – emphasis added). In addition, Hypponen teaches that "the step of defining the database comprises the further steps of updating the database with additional macro signatures" (Col.2, lines 53-55 – emphasis added) and that "[t]his updating may be done via an electronic link between a computer hosting the database (where the scanning of the file is performed) and a remote central computer" (Col.2, lines 55-57).

However, Hypponen's disclosure of determining signatures of macros from end user applications known to be virus free, and compiling the determined signatures into a database which is updated with additional macro signatures, in no way suggests "tailoring said mobile computing device malware definition data to accommodate malware threats to which said mobile computing device is vulnerable" (emphasis added), as claimed by applicant. Clearly, updating a database with determined clean macro signatures, as in Hypponen, simply fails to even suggest "tailoring said mobile computing device malware definition data" let alone where such tailoring is "to accommodate malware threats to which said mobile computing device is vulnerable" (emphasis added), in the manner as claimed by applicant.

Still yet, with respect to the independent claims, the Examiner has relied on the following excerpts from Hypponen to make a prior art showing of applicant's claimed technique "wherein said one or more classes of malware threat against which said mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile computing device, and classes for which it is

desired to protect said mobile computing device according to user defined policies" (see this or similar, but not necessarily identical language in the independent claims).

> "...This updating may be done via an electronic link between a computer hosting the database (where the scanning of the file is performed) and a remote central computer. Alternatively, the database may be updated by way of data stored on an electronic storage medium such as a floppy disk. The database may also include signatures corresponding to widely used proprietary macros, e.g. those used by large organisations." (Col. 2, lines 55-63)
>
> "Preferably, the method comprises creating a set of signatures corresponding to a set of user specific macros, certified by the user as being virus free. These signatures may be added to the first mentioned database, or may be included in a separate database. In either case, the method comprises scanning a macro identified in a file to determine whether or not the macro has a signature corresponding to a signature of a user certified macro. The user in this case may be an end user, but preferably is a network manager. In the latter case, database updates made by the network manager are communicated to the network end user computers where the virus screening is performed." (Col. 3, lines 3-14 - emphasis added)

Applicant respectfully asserts that the excerpts relied upon by the Examiner merely teach that "the method comprises creating a set of signatures corresponding to a set of user specific macros, certified by the user as being virus free," in addition to "scanning a macro identified in a file to determine whether or not the macro has a signature corresponding to a signature of a user certified macro."

However, Hypponen's disclosure of creating signatures corresponding to a set of user specific macros in no way suggests a technique "wherein said one or more classes of malware threat against which said mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile computing device, and classes for which it is desired to protect said mobile computing device according to user defined policies" (emphasis added), as claimed by applicant. Clearly, a database containing signatures of user created virus free macros, as in Hypponen, simply fails to meet "classes for which it is desired to protect said mobile computing device according to user defined policies," or "one or more classes of malware

threat ... chosen according to classes of malware threat known to pose a problem to said mobile computing device" (emphasis added), in the manner as claimed by applicant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Thus, a notice of allowance or a proper prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claim 8 et al., the Examiner has relied on the following excerpt from Lahti to make a prior art showing of applicant's claimed technique "wherein user controlled policy data is used in combination with said threat data to control against which classes of malware threat said mobile computing device is protected by said mobile computing device malware definition data."

> "...to date. A better method is for the user of the mobile device to contact a remote web server operated by the provider of the anti-virus software. The necessary data to update the anti-virus database can then be downloaded from that server." (Paragraph [0021], lines 7-10 - emphasis added)

Applicant respectfully asserts that the excerpt relied upon by the Examiner merely teaches that if a user of a mobile device contacts a remote web server operated by the provider of anti-virus software, then data to update the anti-virus database may be downloaded from the server. However, Lahti's general disclosure of downloading data necessary to update an anti-virus database simply fails to suggest a technique "wherein user controlled policy data is used in combination with said threat data to control against which classes of malware threat said mobile computing device is protected by said mobile computing device malware definition data" (emphasis added), as claimed by applicant. Clearly, downloading updates from a server, as in Lahti, fails to meet "user controlled policy data" or "threat data," in the manner as claimed by applicant.

Again, since at least the third element of the *prima facie* case of obviousness has not been met, a notice of allowance or a proper prior art showing of all of the claim limitations, in the context of the remaining elements, is respectfully requested.

To this end, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P482/01.122.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100